STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

June 14, 2006

The Honorable Laura Knaperek, Chair
Joint Legislative Audit Committee

The Honorable Robert Blendu, Vice Chair
Joint Legislative Audit Committee

Dear Representative Knaperek and Senator Blendu:

Our Office has recently completed a 6-month followup of the Department of Administration—Information Services Division and Telecommunications Program Office regarding the implementation status of the 17 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in September 2005 (Auditor General Report No. 05-11). As the attached grid indicates:

- 17 are in the process of being implemented.

Our Office will continue to follow up at 6-month intervals with the Department on the status of those recommendations that have not yet been fully implemented.

Sincerely,

Debbie Davenport
Auditor General

DD:Acm
Attachment

cc: Bill Bell, Director
Arizona Department of Administration

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. The Department should designate a central authority, such as its state-wide security manager, with the responsibility for developing a comprehensive security program for the Department's internal information resources and network, as well as the data center. The Department should then ensure that the program addresses:	Implementation in Process	
a. Developing a policy governing network scanning, monitoring, and testing, including how it should be done, the frequency, and follow-up procedures to correct identified vulnerabilities;	Implementation in Process	
b. Ensuring that it obtains an independent security assessment at least every 3 years and developing policies regarding the circumstances under which it would obtain an independent assessment more frequently.	Implementation in Process	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
c. Conducting risk assessments at least every 3 years and as needed when systems, facilities, or other conditions change;	Implementation in Process	
d. Developing a system to follow up on identified risks and weaknesses to ensure that they are addressed;	Implementation in Process	
e. Developing adequate security policies and procedures and ensuring that they include sufficient detail; and	Implementation in Process	
f. Providing annual security awareness training as provided for in both GITA and department policy.	Implementation in Process	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
2. The Department should determine if it needs additional staff, funding, and technical resources to perform additional security duties, and if so, assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.	Implementation in Process	
3. The Department should request that the Legislature amend A.R.S. §41-712 to give the Department statutory authority to enforce security requirements for state agencies using AZNET. If the Department receives such authority, it should ensure that it becomes part of its comprehensive security program in conjunction with the first recommendation.	Implementation in Process[1]	

[1] While the Department has not requested statutory authority from the Legislature to enforce security requirements for AZNET, department officials report they are working with the Government Information Technology Agency and the Governor's Office to address this recommendation.

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
4. The Department should enhance its interagency service agreements with state agencies that use the data center to define the Department's and the agencies' security responsibilities. The agreements should:		
a. Delineate the Department's responsibility to provide access to the state data center and the state agency's responsibility to meet specific, minimum security requirements; and	Implementation in Process	
b. Define the circumstances under which a state agency may face actions for failure to comply with those security requirements, and the actions the Department can take to better ensure that corrupted systems in one agency do not compromise other agencies' systems and data.	Implementation in Process	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
5. The Information Services Division should better ensure that it does not publish sensitive information on its Web site by developing a policy requiring central review and approval of Web site content. The Division should also review current Web content to ensure that sensitive information has not remained on its Web site, and instead maintain any sensitive information in a more secure environment, such as the Department's internal network, which is not available to the public.	Implementation in Process	
6. The Department should configure its information system resources, such as routers, switches, and servers, to comply with GITA standards to provide greater safety from external threats.	Implementation in Process	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 2: Improved oversight of telecommunications consolidation and privatized network needed

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. The Department should improve oversight of the inventory process by:	Implementation in Process	
a. Reviewing the TPO's current staffing assignments and reassigning staff to this function or, if necessary,		
b. Reallocating existing resources or taking other steps, as appropriate, to hire a private contractor to adequately oversee the inventory process.		
2. The Department should ensure that the contractor develops an adequate network security plan that includes the following:		
a. Requirements stipulated by the contract, including security service level agreements, compliance with GITA's state-wide security standards, and periodic security awareness and training for agency personnel; and	Implementation in Process	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
6-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 2: Improved oversight of telecommunications consolidation and privatized network needed (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
b. Other relevant aspects of an appropriate information technology security plan, such as defining clear security monitoring and enforcement processes, and how potential security breaches or other incidents will be identified, reported, and monitored.	Implementation in Process	
3. The Department should develop a process for monitoring the contractors and work with them to annually update the security plan to reflect any changes in state-wide network and security standards.	Implementation in Process	